Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) In a public key authentication system, a method of sending an authenticated message to a recipient via a network, the method comprising:

digitally signing a message using a first private key associated with the sender;

retrieving a first certificate reference associated with a first certificate, the first certificate including a first public key corresponding to the first private key, wherein the first certificate and the associated first certificate reference are stored in a public key infrastructure; ~~and~~

transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference;

retrieving a second certificate reference to a second certificate, wherein the second certificate is issued to an issuer of the first certificate, wherein the second certificate and the associated second certificate reference are stored in the public key infrastructure; and

transmitting the second certificate reference as a further portion of the authenticated message.

2. (Original) The method of claim 1, further comprising:

transmitting the first certificate via the network to the public key infrastructure prior to transmitting the authenticated message.

3. (Original) The method of claim 1, wherein the first certificate reference is determined from an identity of the sender and a serial number of the first certificate.

4. (Canceled)

5. (Original) The method of claim 1, wherein the network is the Internet.

6. (Original) The method of claim 1, further comprising encrypting the message using a second public key, wherein the recipient holds a second private key corresponding to the second public key.

7. (Currently Amended) In a public key authentication system, a method for authenticating a message received from a sender via a network, the received message including a digitally signed message, ~~and~~ a first certificate reference and a second certificate reference, the method comprising:

transmitting the first certificate reference to a public key infrastructure via the network;

receiving from the public key infrastructure via the network a first certificate corresponding to the first certificate reference, the first certificate including a first public key;

determining whether the first certificate is trusted; ~~and~~

if the first certificate is trusted, authenticating the digitally signed message using the first public key;

transmitting the second certificate reference to the public key infrastructure via the network; and

receiving from the public key infrastructure a second certificate corresponding to the second certificate reference, the second certificate including a second public key associated with an issuer of the first certificate.

8. The method of claim 7, further comprising:

storing in a local keystore the first certificate reference and the first public key.

9. The method of claim 7, wherein the step of determining whether the first certificate is trusted comprises:

identifying a first issuer of the first certificate;

comparing the first issuer to each of at least one trusted issuer; and

if the first issuer is the same as one of the at least one trusted issuer, determining that the first certificate is trusted.

10. (Canceled)

11. (Currently Amended) The method of claim ~~10~~7, wherein the step of determining whether the first certificate is trusted comprises:

determining whether the second certificate is trusted;

if the second certificate is trusted, using the second public key to authenticate an issuer signature included in the first certificate, thereby verifying the first certificate; ~~and~~

if the first certificate is verified, determining that the first certificate is trusted; and

if the second certificate is not trusted, determining that the first certificate is not trusted.

12. (Original) The method of claim 7, wherein the network is the Internet.

13. (Original) In a public key authentication system, a method for obtaining a public key for

authenticating a received message comprising a digitally signed message and a first certificate reference, the method comprising:

determining whether the first certificate reference is stored within a local keystore;

if the first certificate reference is stored within the local keystore:

retrieving from the local keystore a first public key associated with the first certificate reference; and

if the first certificate reference is not stored within the local keystore:

transmitting the first certificate reference to a public key infrastructure;

receiving from the public key infrastructure a first certificate corresponding to the first certificate reference, the first certificate including the first public key;

determining whether to trust the first certificate; and

adding information to the local keystore, the information including at least the first certificate reference and the first public key.

14. (Original) The method of claim 13, further comprising:

authenticating the digitally signed message using the first public key.

15-19. (Canceled)